

Amendment
Serial No. 10/677,461

Docket 5000-1-504

REMARKS

Reconsideration of the above-identified application in view of the amendments to the claims and the following remarks is respectfully requested.

Claims 1-8 are rejected. Claim 1 is independent claims. Claim 1 has been amended, and claim 2 has been cancelled. New dependent claims 9 and 10 have been added. Support for the new claims can be found at least on page 7, line 20-24 and FIG. 4. No new matter was added. New claim 11 recites feature that was deleted from claim 1.

The specification stands objected to because applicant did not cite cross-references to related patents: 10/659,158 and 10/634,700. In response, applicants have amended the disclosure to provided cross-references to co-pending applications; 10/659,158 and 10/634, 700.

Therefore, applicants respectfully request withdrawal of this ground of rejection.

Claims 1-8 stand rejected under 35 USC § 103(a) as being unpatentable over RFC 2406 IP Encapsulating Security Payload (ESP) published in 1998 (hereinafter "ESP_2406") in view of Brustoloni et al (US 6,963,982).

Claim 1, as amended, now recites a method of transmitting data securely from a source point to a target point in a point-to-multipoint communication network, the method comprising the steps of, inter alia, forming a first integrity check field indicating a CRC (Cyclic Redundancy Check) check sum of the encrypted transmission data; forming a second integrity check field indicating a check sum of the transmission frame and adding the second integrity check field to the transmission frame for a subsequent transmission.

Amendment
Serial No. 10/677,461

Docket 5000-1-504

Claim 1 has been amended to incorporate features cited in claim 2. The Office Action indicates that claim 2 can be easily derived by combining references. However, it is respectfully submitted that references, alone or in combination, do not disclose or suggest checking the integrity of all frames again through the step of "forming a first integrity check field" after checking initially the integrity to an encrypted message and the step "forming a second integrity check field", as recited in base claim 1. The present invention provides a way of identifying whether the received data error is generated when the data is transmitted, or the received data error is generated by an unauthenticated message. These are accomplished by steps cited in base claim 1. The combined references do not anticipate or make the features cited in claim 1 obvious.

Accordingly, applicants respectfully request withdrawal of this ground of rejection.

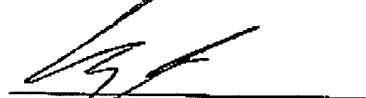
The other claims in this application are each dependent from the independent claim discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual consideration of the patentability of each on its own merits is respectfully requested.

Amendment
Serial No. 10/677,461

Docket 5000-1-504

For all the foregoing reasons, it is respectfully submitted that all the present claims are patentable in view of the cited references. A Notice of Allowance is respectfully requested.

Respectfully submitted,


By: Steve S. Cha
Attorney for Applicant
Registration No. 44,069

Date: May 4, 2007

Steve S. Cha, Reg. No. 44,069
Cha & Reiter, LLC
210 Route 4 East, #103
Paramus, NJ 07652
Telephone: (201) 226-9245
Facsimile: (201) 226-6246